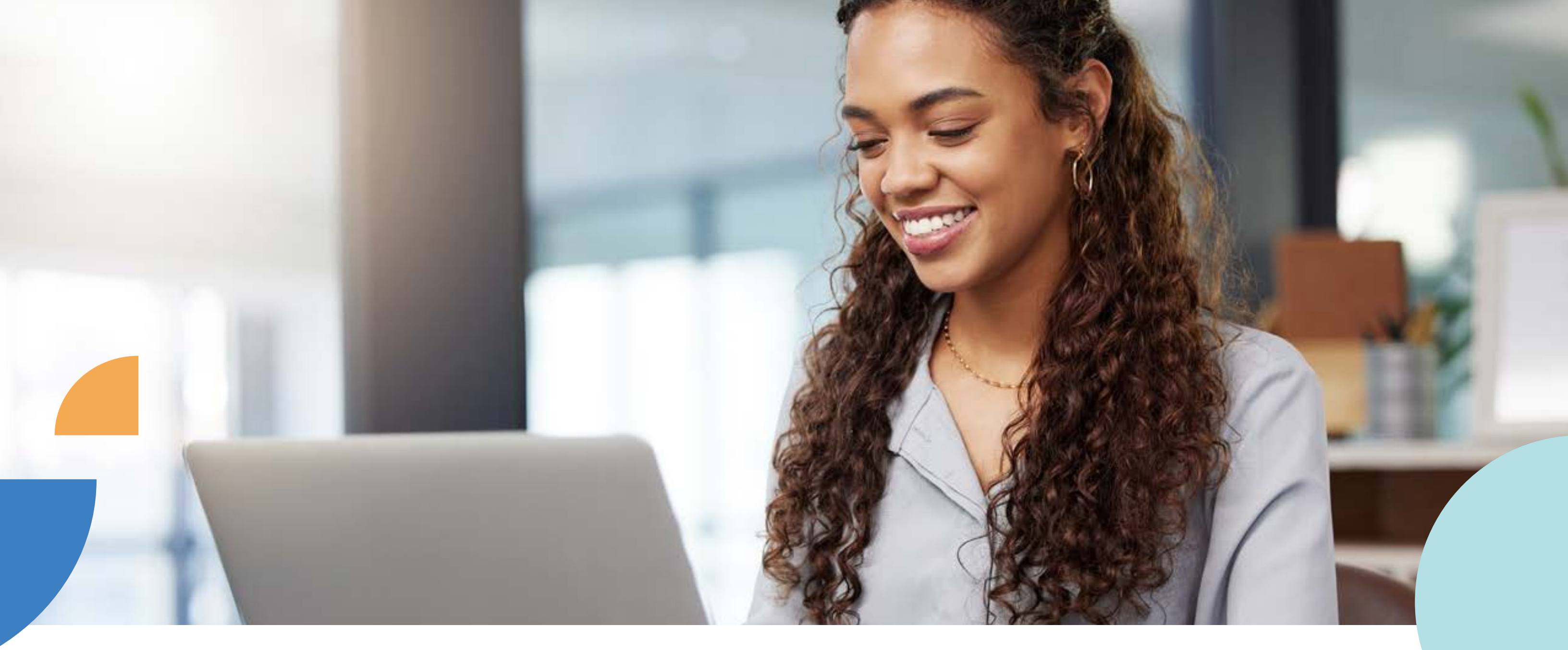
SmartVault

Making Cybersecurity Practical: Cost-Effective, Straightforward Strategies to Implement Today

Whitepaper



Introduction

Cybercrime is a reality for every modern business globally, regardless of size or industry. The accounting profession is particularly hard hit every year, but accounting professionals still underestimate the power of increasing their cybersecurity even though they face severe consequences when their systems are breached. These consequences can include hefty fines, thousands spent recovering lost data, and untold loss of profits due to a battered reputation.

You're likely aware of these consequences—after all, the media coverage about the evolving threat landscape is relentless. If you haven't been affected by a cyberattack, it can be especially tough to carve out time in your busy schedule to implement good cybersecurity practices.

There are many things you can quickly implement to protect your firm now. Taking the time will not only make the busy season more relaxing but will also make your firm more attractive to prospective modern clients who put a big premium on tech security.

In this whitepaper, you'll learn how cybercriminals target accounting firms, what your legal obligations are, and how you can protect your practice and your clients from cyberattacks.

Having strong cybersecurity processes will give you, your staff, and your clients peace of mind that data is protected.

How Do Cybercriminals Hack Accounting Firms?

It's often said, "The best defense is a good offense." The same is true for cybersecurity. Protecting yourself from cybercriminals isn't just about knowing how to safeguard client data from would-be thieves; it's also about being proactive and learning the methods criminals use to infiltrate an accounting practice's systems. We'll go over the four main strategies cybercriminals use below:

Malware

Cybercriminals design malware — short for malicious software — to steal data and destroy and/or damage your computers and systems. Infections typically happen from clicking a link or opening an infected email attachment. Malware includes things like viruses, spyware, and ransomware.

Phishing

This attack lures people into disclosing their personal information, like passwords and Social Security numbers, and it works well. According to the IRS, an estimated 91% of all data breaches and attacks begin with a phishing email. Criminals accomplish this by making the victim believe the message and request are trustworthy. These attempts are usually performed via email or text message and appear to come from known, trusted sources, like your partner, client, bank, loan provider, credit card company, or even places like big-box stores.

Ransomware

That brings us to ransomware. This is a type of malware that makes its victims pay—literally. Ransomware keeps you from accessing your data by encrypting your files, making them unreadable. The criminals give you an ultimatum: Pay up or lose the data indefinitely. Some attackers even demand a second ransom, promising they won't sell your data online to other criminals. Ransomware is a final step in a larger attack, as the criminal already accessed your network and data through an initial method, like malware or phishing.

Man-in-the-Middle (MitM)

Also known as eavesdropping, a perpetrator puts themselves between you and an application (i.e., your mobile device and its Internet browser). The victim is unaware that all the information they're passing to the application goes straight to the perpetrator. The attacker may even install software to access all of your information. People put themselves at risk for this when they connect to the Internet using an unsecure public Wi-Fi.

Creating a Cybersecurity Plan for Your Accounting Firm

As you can see, cyberthieves have many clever ways to steal information. And unfortunately, cybercrime is not only here to stay, but it's on the rise: Some reports suggest attacks now happen every 39 seconds, and the cost of these crimes is expected to skyrocket to $10.5 trillion per year by 2025, up from $6 trillion in 2022.

> **The takeaway:** If you haven't taken the proper steps to protect yourself, it's not a question of if you'll be hacked, but when.

Big and small firms need a plan to avoid becoming a victim. Not only are accounting firm leaders without one risking everything, but they're also breaking the law.

What the Law Says

The Federal Trade Commission requires paid tax and accounting professionals to have a Written Information Security Plan (WISP) that details how they will protect their data. It covers everything from employee training to IT systems and ongoing maintenance requirements. You must have a verified WISP for PTIN renewal.

The Gramm-Leach-Bliley Act (GLBA) requires U.S. financial institutions to protect client data. As the Federal Trade Commission (FTC) implemented GLBA, it also issued the Safeguards Rule—a list of requirements financial institutions must follow.

The FTC requires each financial institution to choose at least one employee to coordinate their information security program. Other requirements include identifying risks to clients' data and evaluating the effectiveness of current safeguarding measures. You also need to create, implement, monitor, and routinely test the safeguarding program, as well as confirm that vendors and service providers maintain appropriate safeguards. Lastly, you should update your plan as regulations, risks, or your business operations change.

Use this checklist to confirm your WISP complies with federal requirements and includes the recommended details.

Download Now

> Cybersecurity is – or at least should be – a paramount concern for any business of any size or industry globally.”
>
> Luke Kiely, SmartVault, CISO

Evaluating Your Risks

There are four main types of weaknesses accounting firm owners need to keep an eye out for:

- **Process vulnerabilities.** These occur when the procedures you’ve implemented to safeguard your system aren’t sufficient. Examples include weak passwords.
- **Network vulnerabilities.** These are problems in your software or hardware that put you at risk of a cyberattack, such as using a Wi-Fi network with weak security.
- **Operating system vulnerabilities.** These are issues with an operating system (OS) that allow hackers to access any device that uses that OS. Not updating your software leaves you at risk of an OS vulnerability.
- **Human vulnerabilities.** Another way to put this is “human error.” This term refers to anything a user does that makes a system vulnerable to attack, and it’s the most common source of weakness. Examples abound; they include things like clicking on an email attachment that’s infected with malware, failing to update an operating system, or storing sensitive information on a server that’s not secure.

As you identify the areas of vulnerability at your accounting firm, make them a top priority to fix. In the next section, we’ll go over some straightforward things you can do right now.

5 Ways to Make Your Accounting Practice More Secure

Transitioning traditional IT infrastructure to the cloud and building in resilient processes is paramount. Here are five things you should do:

1 Know and backup your data

Ensure you know what data you have, where it is stored, and what you consider most sensitive, and apply protections based on the risks you have identified. Luke Kiely, security expert and CISO of SmartVault, advises firm leaders to "think about how much you rely on data in your business, such as customer details, quotes, orders, and payment details. Now, think about how long you would be able to operate without them."

Some best practices include: Avoiding storing data you don't need and consolidating it where possible to make it easier to secure and manage. Where there is a requirement for data to be replicated or cached, ensure that all copies are sufficiently protected. Data that is dispersed (for example, files on users' desktops) can be more accessible for attackers to find and harder to audit.

Regardless of size, all accounting firms should regularly back up their important data. Make sure that these backups are recent and can be restored. By doing this, you're ensuring your practice can still function following the impact of a flood, fire, physical damage, or cyberattack. Furthermore, if you have backups of your data that you can quickly recover, it's harder to be blackmailed by ransomware attacks. Backing up is not at the forefront of everyone's mind—it's easy to forget when you're swamped during tax season, especially. When you use a document management system (DMS) that backs up your data automatically, you don't have to worry about keeping track of doing it yourself.

> It doesn't matter how good your password is if it's not used with other layers of security."
>
> Luke Kiely, SmartVault, CISO

2 Use multi-factor authentication

Despite being widely available, uptake of multi-factor authentication (MFA) is still relatively low. Luke says, "We talk a lot about secure passwords, but the reality is that it doesn't matter how good your password is if it's not used with other layers of security, and a password is not likely to be good enough to secure access to valuable online services by itself."

MFA, including two-factor authentication (2FA), is an extra layer of security for online services. It is becoming a routine, built-in feature for many services, such as email, cloud file storage, and payment methods. It will usually be a case of enabling this feature within the online service. If your service doesn't provide this feature, consider whether you can continue to rely on that service. A password can be easy to steal or guess, and yes, a second factor can also be stolen. But stealing a matching pair is much more difficult.

3 Store everything in the cloud

Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location. You'll also benefit from a high level of availability. Service providers can supply your organization with data storage and web services without you needing to invest in expensive hardware upfront. Choose a provider that offers unlimited storage so you aren't capped on how much your firm can grow.

Better still, a majority of network or cloud storage solutions now allow you to make backups automatically, for instance, by instantly saving new files to a certain folder for you. Using automated backups not only saves time but it also ensures that you have the latest version of your files should you need them.

4 Consider the use of personal devices in the workplace

Mobile technology is an essential part of a modern business. There is so much data being stored on tablets and smartphones every day. What's more, these devices are now as powerful as traditional computers, and because they often leave the safety of the office (and home), they need more protection than "desktop" equipment. In an effort to embrace the ubiquity of technology and to cut down on costs, many accounting firms allow staff to "bring your own device" (BYOD) to work. However, this does pose a security risk.

> Each practice should consider the use of BYOD in the workplace and avoid such solutions becoming permanent without considering how much risk you're willing to accept. After all, BYOD means corporate data is being processed or residing on personal devices.

From a legal perspective, the responsibility for protecting information typically rests with the business, not the device owner. As such, you should understand the relevant data protection laws and regulations for your industry and location, and you need to consider how any commercial or partner agreements are affected by adopting BYOD.

Whatever BYOD approach you take, it is highly recommended that a set of mitigations are implemented to protect data. Luke has a few suggestions, including "setting the minimum services and data available to a personal device, employing strong authentication approaches, and monitoring the service and data being accessed."

He continues, "BYOD approaches which provide little to no visibility or control over personal devices pose the greatest risk to corporate data. Such approaches should only be used where absolutely necessary."

5 Support remote and hybrid work

Staff might feel more exposed to cyber threats when working outside the office environment. Furthermore, don't forget that human error is the source of many vulnerabilities that permit cyberattacks. Make sure your team members know how to report any problems and encourage them to speak up, even if they made a mistake.

Additionally, check how staff are coping, not just in terms of how to use new technologies, but also how they are adapting to having to work in very different ways.

Staff are more likely to have their personal devices stolen (or lose them) when they are away from the office or home. Luke advises firm owners to "[m]ake sure devices encrypt data whilst at rest, which will protect data on the device if it is lost or stolen. Most modern devices have encryption built in, but [it] may still need to be turned on and configured. Fortunately, the majority of devices include tools that can be used to remotely lock access to the device, erase the data stored on it, or retrieve a backup of this data."

Proactively Protect Your Business

Accounting professionals need to embrace cybersecurity and think of it as more than keeping data secure. It has an impact on you, your business, its reputation, your clients, and your staff. Being proactive and having the right tools in place make a big difference. With SmartVault, you'll have a cloud-based document management system and client portal that prioritizes security and compliance and makes it more secure for you, your staff, and your clients to work together online.

Over 30,000 accountants and their clients securely gather, store, share, and eSign documents in the cloud with SmartVault.

Online Document Storage

Standardize and centralize your business documents.

Secure File Sharing

Share files easy, compliant, and secure.

Branded Client Portal

Give clients a professional way to work with you.

Learn more or schedule a demo: www.smartvault.com